State of Indiana Policy and Standards

System Security Plan

Standard ID

IOT-CS-SEC-011

Published Date

7/1/2015

Effective Date

7/1/2015

Last Updated

11/1/2016

Next Review Date

11/1/2017

Policy

09.0 Information Protection Processes and Procedures (PR.IP)

- 09.7 PR.IP-7
  - 09.7.1 Information Protection Metrics and Improvement

Purpose

This Standard summarizes the planning controls in place for the systems with confidential data.

Scope

IOT Supported Entities

Statement

For confidential systems, agencies must develop a Systems Security Plan (SSP). The plan must be:

- Consistent with the State and agency enterprise architecture, describe the operational context of the information system in terms of missions and business processes, provide the security categorization of the information system, describe the operational environment for the information system, describe relationships or connections to other information systems, provide an overview of the security requirements for the system, describe the security controls in place or planned for meeting NIST control requirements, including a rationale for the tailoring and supplementation decisions.
- Formatted based on the State provided templates or latest FedRAMP templates. It shall consider the State of Indiana policies established for confidential systems and include standards, procedures, and other documents supporting operations.
- Reviewed and approved by agency management prior to plan implementation.
- Reviewed annually and updated as changes occur.
- Assessed regularly for compliance with the plan as well as compliance with Policy.
- Updated minimally every three (3) years, to address current conditions or whenever there are significant changes to the information system/environment of operation that affect security.
- Filed with the State CISO and reviewed by the State CIO and cyber security oversight bodies for completeness.
- Categorized as confidential information

Roles

Agency Management

Information Asset Owners/System Owners

Responsibilities

Information Asset Owners/System Owners shall develop, maintain and review on an as needed basis no less than annually for confidential systems.

Management Commitment

Management is responsible for ensuring their agency is keeping up to date with security plans for systems that need them.

Coordination Among Organizational Entities

Agencies shall coordinate with IOT where necessary to understand the requirements related to system security plans and file the latest version.

Compliance

Agencies shall attest to their compliance with these policies on an annual basis providing evidence as directed by the auditor or the CISO.

Exceptions

No exceptions.

Associated Documents

System Security Plan Templates